Using Cisco Network Insights for Resources

This chapter contains the following sections:

Using the Cisco Network Insights for Resources Application

Each node in the fabric streams telemetry data and events to a service in the Cisco NIR app. The Cisco NIR app analyzes the data and detects any anomalies. The Dashboards in the app provide relevant information to view.

Cisco NIR Dashboard

The Cisco Network Insights for Resources (Cisco NIR) application main dashboard provides immediate access to anomalies occurring in the network. Anomalies are learned deviations from the last known "good" state of a switch and are displayed by type and severity. Anomalies include resource utilization, environmental, and interface-level errors, and are color coded based on severity:

- Critical: Red
- Major: Orange
- Minor: Yellow
- Warning: Turquoise
- Information: Blue
- Healthy: Green

Dashboard Inventory

Anomalies are raised when a certain parameter threshold exceeds, or a rate of change threshold exceeds. The main dashboard displays the following information.

Property	Description
Fabric Anomaly Score	Displays the health of the fabric through color.
Spines	Displays the total number of spine nodes in the fabric with anomalies.

Property	Description
Leafs	Displays the total number of leaf nodes in the fabric with anomalies.

Click Spines and Leafs to view the details of the individual nodes in the fabric from Browse Nodes work pane.

Browse Nodes

The Browse Nodes pane displays the graph with top nodes based on Resource Utilization, Environmental, Statistics, End Point Analytics, and Flow Anamoly, which are various ways of viewing the behavior of the nodes. The page also dispalys the overview of the individual nodes in the fabric with node name, switch models, node type and other details. Click **Node** for the node detail view. The **Node Overview** section dispalys the top five nodes based on Resource Utilization, Environmental and Flow analytics with the break down of the faults and events. The **Anomalies** section displays the anomalies that the system detects.

The Browse Nodes pane displays the graph with top nodes based on Resource Utilization, Environmental, Statistics, and Flow Analytics, which are various ways of viewing the behavior of the nodes. The page also dispalys the overview of the individual nodes in the fabric with node name, switch models, node type and other details. Click the **Node** for the node summary pane to display all the gathered information for the selected node.

Click the ↗ icon on the right top corner of the summary pane to show the **Node Details** page. The Node Details page displays General Information, Node Overview, and Anomalies. The **Node Overview** section dispalys the top five nodes based on Resource Utilization, Environmental, and Flow analytics with the break down of the faults and events. The **Anomalies** section displays the anomalies that the system detects.

On the detail page for the selected node, click the ellipses (•••) icon on the right top navigation pane for additional related information for the node such as, Flows, Statistics, Resources, Anomalies, Events, and Environmental Resources.

From the ellipses menu click **Flows for the node** to open **Browse Flows** work pane, which filters the flows to view the top nodes by flow anomalies. Click **Statistics for the node** to open **Browse Statistics** pane, which filters the flows to view the top nodes by interface utilization.

Dashboard Anomalies

The main dashboard displays the anomalies detected in the fabric nodes.

Property	Description
Anomalies by Type	Displays the number of Anomalies by their type. Anomaly types include: • Flow Analytics • Utilization • Environmental • Statistics

Property	Description
Anomalies by Severity	Displays the number of Anomalies (internal Fabric failures) and their severity level. Clicking on the area shows detail fault information, such as **Node** and **Anomaly Score**. • Critical • Major • Minor • Info

Click any number from Anomalies by Type and Anomalies by Severity to access the Browse Anomalies work pane.

Browse Anomalies

The Browse Anomalies pane displays the graph with top nodes by anomaly score based on Type and Severity. The page also dispalys the overview of the individual nodes in the fabric with severity, resource type, node name, acknowledged and other details. Double-click the anomaly for the anomaly details. The **Anomaly Details** page displays the general information of the anomaly, anomalies, list of paths, and related details.

On the **Anomaly Details** page for the selected node, click the ellipses (⋯) icon on the right top navigation pane for additional related information for the node such as, Flows, Statistics, Resources, Anomalies, and Environmental Resources.

From the ellipses menu click **Flows for the node** to open **Browse Flows** work pane, which filters the flows to view the top nodes by flow anomalies. Click **Statistics for the node** to open **Browse Statistics** pane, which filters the flows to view the top nodes by interface utilization.

Browse Anomaly Filters

The Cisco Network Insights for Resources, application dashboard provides immediate access to anomalies occurring in the network. View, sort, and filter anomalies through the Browse Anomalies work pane.

You can refine the displayed anomalies by the following filters:

- Start Time - Display only anomalies with a specific start time.
- End Time - Display only anomalies with a specific end time.
- Description - Displays additional information about the anomaly.
- Node - Display only anomalies for specific nodes.
- Category - Display only anomalies from a specific categary.
- Resource Type - Display only anomalies of a specific resource type.
- Severity - Display only anomalies of a specific severity.
- Acknowledged - Do not display the selected anomaly when checked to **T** for 20 minutes.

As a secondary filter refinement, use the following operators:

- = = - with the initial filter type, this operator, and a subsequent value, returns an exact match.

- != - with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
- contains - with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- !contains - with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

Property	Description
Start Time	The start time stamp for the anomaly detection.
End Time	The end time stamp for the anomaly detection.
Severity	The current severity level of the event. The levels are: • **Critical**—A service-affecting condition that requires immediate corrective action. For example, this severity could indicate that the managed object is out of service and its capability must be restored. • **Major**—Serious problems exist with one or more components. These issues should be researched and fixed immediately. • **Minor**—Problems exist with one or more components that might adversely affect system performance. These issues should be researched and fixed as soon as possible before they become a critical problem. • **Other**—Potential problems exist with one or more components that might adversely affect system performance if they are allowed to continue. These issues should be researched and fixed as soon as possible before they become a critical problem.
Resource Type	The resource type such as **Flow**, configuration, or operational.
Nodes	The node where the anomaly occurred.
Description	Additional information about the anomaly.

Cisco NIR System

The System section of the NIR application contains two areas of data collection:

- **Resource Utilization**—Fabric component capacity information.
- **Environmental**—Hardware component capacity information.

System Resource Utilization

The System Resources of the Cisco NIR application contains two areas of data collection.

Resource Utilization Dashboard

The Resource Utilization dashboard displays utilization, rate of change, trends, and resource anomalies over time for operational, configuration and hardware resources. Top leaf and spine nodes are displayed based on the factors that produced the high utilization.

Property	Description
Top Nodes by Capacity	The leaf node observations search can be more refined by filtering the information by the top leaf nodes.
Node Details	Displays the node trend observations by resource type: • Operational Resources • Configuration Resources • Hardware Resources

Browse Resource Utilization

View, sort, and filter statistics through the Browse Resource Utilization work pane.

Filters

You can refine the displayed statistics by the following filters:

- Node - Display only nodes.

As a secondary filter refinement, use the following operators:

- = = - with the initial filter type, this operator, and a subsequent value, returns an exact match.
- != - with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
- contains - with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- !contains - with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

Property	Description
Top Nodes by	Displays the top nodes by: • MAC • IPv4 Host Routes • IPv6 Host Routes • IPv4 Prefix Routes • IPv6 Prefix Routes • Multicast Routes • VLAN • VRF • Port Usage • Ingress Port Bandwidth • Egress Port Bandwidth • CoPP • LPM • HRT • L2 QoS TCAM • L3 QoS TCAM • VTEP • VNI L2 • VNI L3 • VLAN • Ingress VLAN ACL • Egress VLAN ACL • Ingress Port ACL • Ingress Routed ACL • Egress Routed ACL

Property	Description
Operational Resources	Displays a list of operational resources based on anomaly score. List information includes: • Anomaly Score • Node • MAC • IPv4 Host Routes • IPv6 Host Routes • IPv4 Prefix Routes • IPv6 Prefix Routes • Multicast Routes
Configuration Resources	Displays a list of configuration resources based on anomaly score. List information includes: • Anomaly Score • Node • VLAN • VTEP • VNI • L2 • L3 • VRF

Property	Description
Hardware Resources	Displays a list of configuration resources based on anomaly score. List information includes: • Anomaly Score • Node • Port Usage • Port Bandwidth • CoPP • LPM • HRT • QoS TCAM • L2 • L3 • VLAN ACL • Ingress • Egress • Port ACL • Ingress • Egress • Routed ACL • Ingress • Egress

System Environmental

The System Environmental of the Cisco NIR application contains two areas of data collection.

Environmental Dashboard

The Environmental Dashboard displays utilization, rate of change, trends, and anomalies over time for switch environmental resources such as fans, power, CPU, and memory.

Property	Description
Top Nodes by Utilization	Displays the percentage utilized per component: • CPU • Memory • Temperature • Fan Utilization • Power Supply • Storage
Node Details	Displays the node trend observations by environmental resource type.

Browse Environmental Resources

View, sort, and filter statistics through the Browse Environmental Resources work pane.

Filters

You can refine the displayed statistics by the following filters:

- Node - Display only nodes.

As a secondary filter refinement, use the following operators:

- = = - with the initial filter type, this operator, and a subsequent value, returns an exact match.
- != - with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
- contains - with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- !contains - with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

Property	Description
Top Nodes by	Displays the top nodes by: • CPU (percent utilization) • Memory (percent utilization) • Temperature • Fan Utilization • Power Supply • Storage

Cisco NIR Operations

The Operations section of the Cisco NIR application contains two areas of statistical and analytical information:

- **Statistics Analytics**—Switch nodes interface usage and protocol statistics.
- **Flow Analytics**—Telemetry information collected from various devices in the Cisco ACI fabric to the NX-OS fabrics.

Statistics Analytics

The Operations Statistics section of the Cisco NIR application contains interface and protocol statistical information for top switch nodes.

Statistics Dashboard

The Statistics Dashboard displays top switch nodes by interface errors or usage, and protocol statistics.

Property	Description
Top Nodes by Interface Utilization	Displays the top nodes based on the combined bandwidth utilization of it's interfaces.
Top Nodes by Interfaces	Displays the top nodes and lists the transmit and receive bandwidth utilization of each of it's interfaces.

Browse Statistics Filters

Browse Statistics filters the interfaces to visualize the top interfaces by anomalies through the Browse Statistics work pane.

You can view, sort, and filter statistics through the Browse Statistics work pane. You can refine the displayed statistics by using the following filters:

- Node - Display only nodes.
- Interface - Display only interfaces.
- Protocol - Display only protocols.

As a secondary filter refinement, use the following operators:

- = = - with the initial filter type, this operator, and a subsequent value, returns an exact match.
- != - with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
- contains - with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- !contains - with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

Property	Description
Top 10 Interfaces by	Displays the top interfaces by: • Transmit Utilization • Receive Utilization • Error
Interface Statistics	Displays a list of interface statistics based on anomaly score. List information includes: • Anomaly Score • Interface • Node • Type • Receive Utilization • Transmit Utilization • Errors
Protocol Statistics	Displays a list of protocol statistics based on anomaly score. List information includes: • Node • Type • Protocol • Number of Interfaces • Errors

Note In order for the Cisco NIR app to receive data from the nodes, confirm that all the nodes in the fabric are synced with PTP Grand master for hardware telemetry and NTP clock for software telemetry.

Browse Statistics

The Browse Statistics dashboard displays interface statistics and protocol statistics for the top interfaces by anomalies for nodes.

Interface Statistics

The Browse Statistics dashboard displays interface statistics for the top interfaces by anomalies for nodes that are of type - physical, port channel, and virtual port channel (PC and vPC) interfaces.

The green dot next to the interface name represents the operational status that the interface is active. The red dot next to the interface name represents that the interface is down.

The interface type is physical, port channel, or virtual port channel (PC or vPC) interface. Double-click **type** > **physical** for interface details of the node such as, node name, physical interface name, operational status, and admin state. The page also displays protocols, QoS, and DOM properties of the physical interface.

The port channel is an aggregate of physical interfaces and they can be statistically chaneled or can be dynamic using LACP protocols. The statistical data that collects the counters for packets, bytes and various errors are similar to that of physical interface. The sourceName differentiates the physical interface from port-channel (aggregated interfaces). The operational data is obtained by looking at additional set of objects that gives the admin-status, oper-status and list of member interfaces for both PC and vPC.

Click **type** > **pc** for interface details of the node such as, node name, port channel name, operational status, and admin state. The page also displays the anomalies, traffic, and member interfaces associated in the port channel.

The vPC is a logical interface that spans accross two physical switches for fault tolerance. Double-click **type** > **vpc** for interface details of the node such as, node name, virtual port channel name, domain id, operational status, and admin state. The page also displays the anomalies, traffic, and the member interfaces associated in the nodes that are in the virtual port channel.

Protocol Statistics

The Browse Statistics dashboard displays protocol statistics for the top interfaces by anomalies for nodes that are of type CDP, LLDP, LACP, and BGP protocol. This page also displays node name and **Count** - the number of interfaces that the protocol is using or the number of sessions that the protocol is using for the node.

The BGP protocol data can be classified broadly into operational and statistical data. The operational data comprises of additional set of objects that gives the admin-status, oper-status and list of VRFs and VRF level information such as vrfName, vrfOperState, vrfRouteId, list of address family associated with each VRF, and list of peer and peer-entry information associated with each VRF. The statistical data comprises of peer-entry counters such as number of open's, updates, keepalives, route-refresh, capability, messages, notifications and bytes sent and received. It also includes peer-entry address family level the route count.

Double-click **protocol** > **BGP** for protocol details of the node such as, node name, protocol name, admin state, operational state and additional details. This page also displays the anomalies, neighbor nodes that are active, errors in the node, neighbor IP address, details about the established neighbors and not connected neighbors that the BGP protocol is using from the node family. Double-click a **Neighbor** node for the **Neighbor Details** window to popup with more details.

Double-click **protocol** > **CDP**, **protocol** > **LLDP**, or **protocol** > **LACP** for protocol details of the node such as, node name, protocol name, anomalies, interfaces that are active, errors in the node, and more details of the interface.

Flow Analytics

The Flow Analytics section of the Cisco NIR application displays the anomalies detected in the flow such as average latency, packet drop indication, and flow move indication collected from various nodes in the fabric.

Flow Analytics Overview

Flow Analytics provides deep insights at a flow level giving details such as average latency, packet drop indicator and flow move indicator. It also raises anomalies when the latency of the flows increase or when packets get dropped because of congestion or forwarding errors.

Each flow has a packet counter representing the number of packets entering the ASIC for that flow over a period of time. This period of time is called aggregation interval. There are several points where flow statistics for a given flow can be aggregated. Aggregation can happen in the ASIC, switch software, and server software.

Flow Analytics Hardware Requirements

Flow Analytics for Cisco NIR application in Cisco DCNM require the following hardware:

- For details on Flow Telemetry support for Cisco Nexus series switches, see Hardware Requirements.

Flow Analytics Limitations

The following are limitations for Flow Analytics for Cisco NIR application on Cisco Nexus EX line cards. For details on Flow Telemetry hardware support, see Hardware Requirements.

- Output port information for outgoing traffic from N9K-C93180YC-EX, N9K-C93108TC-EX, and N9K-C93180LC-EX line cards will not be displayed.

Flow Analytics Dashboard

The Flow Analytics Dashboard displays telemetry information collected from various devices in the fabric. The flow analytics records let the user visualize the flows in the fabric and their characteristics across the entire Cisco DCNM fabric.

Property	Description
Top Nodes by	The flow analytics engine also runs machine-learning algorithms on the behavior of the flows to raise anomalies in the behavior, such as Average Latency, Packet Drop Indicator, and Flow Move Indicator. The graph represents the anomalies in the behavior over a period of time.
Top Nodes by Flow Anomalies	Flow telemetry and analytics gives in-depth visibility of the data plane. The flow analytics engine collects the flow records streamed from the ASIC hardware and converts the 5-tuples to user-understandable flow records. Top nodes by flow anomalies displays the nodes in the network with the most anamolies. The details include, type of alarm, source destination, packet drops and latency.

In the **Top Nodes by Flow Anomalies** click the node card to display the Brows Flows page.

Browse Flows

The Browse Flows page dispalys the active nodes, ingress nodes, egress nodes, and flow collection filters, which display the anomalies in the fabric nodes.

Property	Description
Top 10 flows by	Lists the top 10 flows that scored highest in the following: • **Anomaly Score**—The score is based on the number of detected anomalies logged in the database. • **Packet Drop Indicator**—The flow records are analyzed for drops. The primary method of detecting drops is to check for discrepancies in the ingress and egress packet counts. • **Latency**—The time taken by a packet to traverse from source to destination in the fabric. **Note** A prerequisite for fabric latency measurement is that all the nodes shall be synchronized with uniform time. • **Flow Move Indicator**—The number of times a Flow moves from one Cisco DCNM leaf switch to another. The first ARP/RARP or regular packet sent by that endpoint appears as a flow entering the fabric through the new Cisco DCNM nodes.
Browse Flows	Displays the following properties for the top nodes by flow anomalies: • Anamoly Score—Displays the health state of the nodes. • Original Timestamp—Diaplays the timestamp when the anomaly occurred. • Nodes—Active nodes that show the anomaly score. • Ingress—Dispalys the Ingress switch name and VRF that show the flow anomalies. • Egress—Dispalys the Egress switch name and VRF that show the flow anomalies. • Source—Displays the VLAN, VNI, source address, and port information of the nodes by flow anomalies. • Destination—Displays the VLAN, VNI, destination address, and port information for the nodes by flow anomalies. • Address Type—Displays the address type as IPV4 or IPV6. • Protocol—Displays the protocol for the flow anomaly nodes. • Packet Drop Indicator—Displays the packet drops for the nodes. • Latency—Displays the latency information for the nodes. • Flow Move Indicator—Displays the packet flow moves for the nodes.

Double click the anomaly for the flow details. The **Flow Details** page displays the general information of the anomaly, anomalies, path summary, anomaly charts, and related details.